

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

## Interview

## Overview

Claim 13 of the subject application recites “content on [a] removable storage medium,” “obtaining the one or more keys from the removable storage medium,... wherein the one or more keys are for decrypting content on the removable storage medium” and “communicating the one or more keys to the remote client computing device.” Thus, the keys communicated to the client are

1 obtained from the removable storage medium that also contains the content. Spies  
2 et al. do not teach the foregoing. The claim further recites that “the one or more  
3 keys from the DVD [are] also usable to verify authenticity of the DVD drive.”  
4 There is nothing in the Spies et al. patent that teaches this concept either. Further  
5 discussion of the claims and the rejections asserted in the current Office Action is  
6 provided below.

### 8 **Claim Rejection Under 35 U.S.C. §§ 102 & 103**

9 Claims 13, 17-18, 19-21, 23-25 and 27-28 stand rejected as being  
10 anticipated under §102 in view of US Patent 6,055,314 to Spies et. al (hereinafter  
11 “Spies”). Claims 1, 3, 4 and 6-11 stand rejected as being unpatentable under §103  
12 over Spies in view of U.S. Patent 6,272,283 to Nguyen. Claims 2, 12, 14, 15, 16,  
13 26 and 29 stand rejected as being unpatentable under §103 over Spies and Nguyen,  
14 and further in view of Powerfile C20 FAQs (hereinafter “Powerfile”). Finally,  
15 claims 5 and 22 stand rejected under §103 over Spies in view of a description of  
16 DirectShow ([www.compressionworks.com](http://www.compressionworks.com)). These rejections are respectfully  
17 traversed.

18 Spies discloses a system in which a customer, when purchasing a DVD or  
19 otherwise purchasing video content, also receives “decryption capabilities” from  
20 the vendor of the DVD. In the case of purchasing a DVD, the decryption  
21 capabilities are placed on an IC card that is carried by the user. In one described  
22 scenario, the user presents the IC card to the vendor when purchasing the DVD,  
23 and the vendor transfers the decryption capabilities to the IC card. (*Column 6,*  
24 *lines 11-33.*) The decryption capabilities can include a “program key.” In another  
25 scenario, the decryption capabilities can be obtained via network and then stored

1 on the IC card. (*Column 6, lines 34-58.*) Once the decryption capabilities are in  
2 the IC card, the IC card is used in conjunction with a playback device to decrypt  
3 the purchased DVD or other video content.

4 Before the above can occur, according to Spies, a video merchant performs  
5 an initial transaction with a video content provider. The video content provider  
6 maintains a video program storage 30 and a program keys database 32. The video  
7 program storage 30 has a plurality of video content programs that the video  
8 merchant might want to sell. The program keys database 32 includes a number of  
9 program keys that enable use of the video content programs stored in the program  
10 storage 30. (*Column 5, lines 10-18.*) The video merchant contacts the video  
11 content provider to obtain video content and keys that will enable use of the  
12 obtained video content.

13 The process of obtaining video content and associated keys is summarized  
14 in the following. In one example, the video merchant obtains video content that is  
15 for resale. At this point, the video content cannot be played/consumed. The video  
16 content may be sent to the video merchant over a distribution network, or may be  
17 delivered to the merchant on portable media, such as digital video disks. (*Column*  
18 *5, lines 25-32.*) The video content, whether delivered via network or by way of  
19 portable media, is not sent with enabling playback keys that may be used to enable  
20 playback of the video content.

21 The video merchant is now ready to accept keys that will enable video  
22 content that the merchant is authorized to sell. (*Column 5, lines 36-39.*) Spies  
23 gives several examples as to how these keys can be conveyed to the video  
24 merchant. One way is over a secure or insecure link, where the keys are conveyed  
25 in encrypted form. (*Column 5, lines 40-43.*) Spies also mentions that the keys

1 may be "ported on a floppy disk" to the merchant (*Column 5, lines 43-44.*) The  
2 Office is earnestly requested to keep the foregoing sentence in mind when  
3 considering the remainder of this Response. The reasoning being that Spies is  
4 porting *only* keys on floppy disk, not keys *and* the video content that the keys  
5 enable.

6 The Spies et al. patent is also silent regarding the additional subject matter  
7 added to claims 1, 13 and 19.

8 It is respectfully submitted that the mechanisms described by Spies do not  
9 include the elements recited by the claims.

10 **Independent claim 13** recites "content on [a] removable storage medium,"  
11 "obtaining the one or more keys from the removable storage medium,... wherein  
12 the one or more keys are for decrypting content on the removable storage medium  
13 and for verifying authenticity of the DVD drive" and "communicating the one or  
14 more keys to the remote client computing device." Thus, the keys communicated  
15 to the client are obtained from the removable storage medium that also contains  
16 the content.

17 Spies does not disclose this. The Office maintains the Spies disclosure  
18 found at column 5, lines 35-45, column 6, lines 34-58, column 13, lines 24-30,  
19 column 4, lines 35-53, column 12, lines 25-30, and column 9, lines 9-11 teaches  
20 the limitations indicated from claim 13. The Applicant disputes this conclusion  
21 for the following reasons.

22 Column 5, lines 35-45, teaches that keys are delivered to a video merchant  
23 to enable use of video content. As discussed above, this is done over a network or  
24 via disk. However, the delivery of the keys does not include delivery of the video  
25 content that the keys enable. To do this would defeat the purpose of the Spies

1 system; Spies wants to keep the keys and the video content separate to protect  
2 against unauthorized interception of video content. (*Column 16, lines 55-67.*)  
3 Therefore, this section of Spies does not teach or suggest at least “obtaining the  
4 one or more keys from the removable storage medium,... wherein the one or more  
5 keys are for decrypting content on the removable storage medium.”

6 Column 6, lines 34-58, teaches how a user can go about purchasing video  
7 content from a video merchant and enabling the purchased video content for  
8 playback. In this example, the user selects and receives the video content over a  
9 network. However, the video content is not received in a format that is enabled  
10 for viewing. The user receives a key that enables viewing of the video content  
11 separately. The key is not sent with the video content, nor is the key associated  
12 with the video content. As was discussed earlier, the video content and the keys  
13 are kept separately. The video content is stored on a storage 30, and the keys are  
14 stored in a database 32. Therefore, this section of Spies does not teach or suggest  
15 at least “obtaining the one or more keys from the removable storage medium,...  
16 wherein the one or more keys are for decrypting content on the removable storage  
17 medium.”

18 Column 13, lines 24-30, teaches particulars of a video purchasing  
19 application 168 that may be used to purchase video content available for purchase  
20 from the video merchant. Nothing in this section of Spies even remotely  
21 approaches the indicated limitations of claim 13.

22 Column 4, lines 35-53, encompasses part of the Brief Description of the  
23 Drawings section and one paragraph of the detailed description. This section  
24 states, for context, that a reader of the Spies document is assumed to have  
25

1 knowledge of basic cryptography. As with the other sections discussed above,  
2 nothing in this section teaches or suggests the indicated limitations of claim 13.

3 Column 12, lines 25-30, teaches that generated keys are intended for  
4 “sessional” use. This means that a key generated for a particular video content is  
5 not used for another particular video content. As a matter of fact, this section of  
6 Spies indicates that a key is destroyed after it is distributed to an authorized  
7 customer. This section makes no mention of where the keys are coming from.  
8 Moreover, the section does not reference a source of the video content. Therefore,  
9 there is nothing in this section that teaches or suggests “obtaining the one or more  
10 keys from the removable storage medium,... wherein the one or more keys are for  
11 decrypting content on the removable storage medium.”

12 For the reasons discussed above, Spies fails to disclose every element of  
13 claim 13, and the §102 rejection of claim 13 is invalid. Allowance of claim 13 is  
14 respectfully requested.

15 **Dependent claims 14-18** are allowable because of their dependence from  
16 allowable base claim 13, and also for their additionally recited elements.  
17 Although claims 14-16 are rejected as being obvious over a combination of Spies,  
18 Nguyen and Powerfile, Nguyen and Powerfile do not describe the elements  
19 discussed above that are absent from Spies. Therefore, the arguments above apply  
20 as well to claims 14-16; Powerfile and Nguyen are not asserted by the Office to  
21 suggest transferring keys from the storage medium itself.

22 **Independent claim 19** recites “a key exchange process with a disc drive in  
23 order to decode media content on a disc accessible to the disc drive.” In addition,  
24 claim 19 recites “communicating . . . one or more keys from the disc that can be  
25 used at the computing device to decode the particular media content, the one or

1 more keys form the disc also usable to verify authenticity of the disc drive.” Spies  
2 does not disclose this subject matter. Again, the Office relies on the passages  
3 discussed above in connection with the rejection of claim 13. However, these  
4 passages of Spies do not mention, teach or suggest the concept of obtaining a key  
5 from “the disc that can be used at the computing device to decode the particular  
6 media content,” where the disc originating the key also contains content that can  
7 be decoded with the key.

8 Allowance of claim 19 is therefore requested.

9 **Dependent claims 20-23** are allowable because of their dependence from  
10 allowable base claim 19, and also for their additionally recited elements. Although  
11 claim 22 is rejected as being obvious over a combination of Spies and DirectShow,  
12 DirectShow does not describe the characteristics indicated above that are absent  
13 from Spies. Therefore, the arguments above apply as well to claim 22.

14 **Independent claim 24** recites a server component, and a DVD drive on the  
15 server component. In addition, claim 24 recites that the server component  
16 “operates as an intermediary between a DVD player on the client component and a  
17 DVD drive on the server component.” Again, Spies does not show this.

18 In addressing this element, the Office relies upon Spies at col. 12, lines 8-  
19 53. This portion of Spies describes various details relating to key exchange, and  
20 starting at line 39, describes how a viewer decrypts video from a distribution  
21 medium. The decryption involves the “viewer computing unit,” the IC card, and a  
22 DVD reader. However, Spies does not describe a server component that has a  
23 DVD drive and that “operates as an intermediary between a DVD player on the  
24 client.” The Office has not indicated any proposal for how the components of  
25

1 Spies might be correlated to the elements recited in claim 24, and the Applicant  
2 does not believe any reasonable correlation exists.

3 Accordingly, it is believed that claim 24 is allowable.

4 **Dependent claims 25-26** are allowable because of their dependence from  
5 allowable base claim 24, and also for their additionally recited elements.  
6 Although claim 26 is rejected as being obvious over a combination of Spies,  
7 Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics  
8 indicated above that are absent from Spies. Therefore, the arguments above apply  
9 as well to claim 26; Nguyen and Powerfile are not asserted by the Office to  
10 suggest "an intermediary between a DVD player on the client component and a  
11 DVD drive on the server component."

12 **Independent claim 27** recites a server component configured to "exchange  
13 Content Scrambling System (CSS) keys between a DVD drive of the system and  
14 the key exchange client component." Spies does not describe exchanging keys  
15 between a DVD drive and any other component.

16 In rejecting claim 27, the Office states that this element is addressed by  
17 Spies at col. 12, lines 8-53. Within these lines, however, Spies only discusses a  
18 DVD drive at lines 49-53. And within lines 49-53, Spies does not discuss  
19 exchanging keys with a DVD drive.

20 Accordingly, Spies does not show every element of claim 27, and should be  
21 allowed.

22 **Dependent claims 28-29** are allowable because of their dependence from  
23 allowable base claim 27, and also for their additionally recited elements.  
24 Although claim 29 is rejected as being obvious over a combination of Spies,  
25 Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics



1 indicated above that are absent from Spies. Therefore, the arguments above apply  
2 as well to claim 29; Nguyen and Powerfile are not asserted by the Office to  
3 suggest exchanging keys between a DVD drive . . . .”

4 **Independent claim 1** recites a server device having a “DVD drive,” and a “  
5 key exchange server.” A client device has “a key exchange client and a decoder”.  
6 Claim 1 further recites that the “key exchange client and the key exchange server  
7 communicate with one another to pass one or more keys *from the DVD* to the key  
8 exchange client to allow the decoder to decrypt *content* received, via the network,  
9 *from the DVD*, the one or more keys from the DVD also usable to verify  
10 authenticity of the DVD drive.” Spies does not disclose passing one or more keys  
11 from a DVD. Nor does Spies does teach or suggest the concept of decrypting  
12 content received over a network using a key, where the key and the content come  
13 from the same source (i.e., the DVD). Further more, Spies does not teach or  
14 suggest that the one or more keys from the DVD are also usable to verify  
15 authenticity of the DVD drive.

16 In addressing the element of claim 1, the Office references column 3, lines  
17 40-45 of Spies. This paragraph states that a content provider supplies an  
18 encrypted video stream on a network or DVD. The last sentence of the paragraph  
19 states that decryption is performed at the client by using the decryption capabilities  
20 of the IC card. Lines 40-45 do not discuss keys other than the “stored program  
21 key” held by the IC card. There is no description of any keys being transferred  
22 “from the DVD” to a client.

23 In addressing the element of claim 1 further, the Office references column  
24 6, lines 55-58. This portion of Spies is discussed in detail earlier in this Response.  
25 There is nothing in this portion of Spies that teaches or suggests passing “one or

1 more keys *from the DVD* to the key exchange client to allow the decoder to  
2 decrypt *content* received, via the network, *from the DVD*.”

3 The Office admits that Spies fails to teach or suggest “passing the  
4 cryptographic keys from the DVD to the key exchange client,” and relies upon  
5 Nguyen to make up for this deficiency. However, there is nothing in Nguyen that  
6 can remedy the Spies deficiency discussed in detail herein. In particular, the  
7 combination of Spies in view of Nguyen does not teach or suggest at least passing  
8 “one or more keys *from the DVD* to the key exchange client to allow the decoder  
9 to decrypt *content* received, via the network, *from the DVD*.”

10 Accordingly, Spies fails to disclose every feature of claim 1, and the §103  
11 rejection of claim 1 is unfounded. Withdrawal of the rejection is respectfully  
12 requested.

13 **Dependent claims 2-12** are allowable because of their dependence from  
14 allowable base claim 1, and also for their additionally recited elements. Although  
15 claims 2 and 12 are rejected as being obvious over a combination of Spies,  
16 Nguyen and Powerfile, Nguyen and Powerfile do not describe the characteristics  
17 indicated above that are absent from Spies. Therefore, the arguments above apply  
18 as well to claims 2 and 12; Nguyen and Powerfile are not asserted by the Office to  
19 suggest transferring keys from the storage DVD. Although claim 5 is rejected is  
20 rejected as being obvious over a combination of Spies and DirectShow,  
21 DirectShow does not describe the characteristics indicated above that are absent  
22 from Spies. Therefore, the arguments above apply as well to claim 5.

23 Addition **independent claim 30** recites the subject matter “the key  
24 exchange client and the key exchange server communicate with one another keys  
25 from the DVD to the key exchange client, at least one of the keys to allow the

1 decoder to decrypt content received, via the network, from the DVD, and another  
2 of the keys is specific to a media content player incorporating the decoder, and  
3 wherein the server component obtains, based on information received from the  
4 client component, an appropriate key for the media content player.” This subject  
5 matter is neither taught nor suggested by any of the documents relied upon by the  
6 Office. Therefore, it is respectfully submitted that this claim is in condition of  
7 allowance.

8  
9 **Conclusion**

10 All claims are in condition for allowance. Applicant respectfully requests  
11 prompt allowance of the subject application. If any issue remains unresolved that  
12 would prevent allowance of this case, **the Examiner is requested to contact the**  
13 **undersigned attorney to resolve the issue.**

14  
15 Respectfully Submitted,

16  
17 Date: 12/16/05

18 By: Tim R. Wyckoff  
19 Tim R. Wyckoff  
20 Lee & Hayes, pllc  
21 Reg. No. 46,175  
22 (206) 315-4001 ext. 110  
23  
24  
25